08-10-00

A

Please type a plus sign (+) inside this box [+]

PTO/SB/05 (2/98)

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for nonprovisional applications under 37 CFR § 1.53(b))

Attorney Docket No.	500122.02
First Inventor or Application Identifier	Hoyt A. Fleming, III
Title	METHOD AND SYSTEM FOR FILTERING UNAUTHORIZED ELECTRONIC MAIL MESSAGES
Express Mail Label No	EL476400477US

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: Box Patent Application
Assistant Commissioner for Patents
Washington, D.C. 20231

1. ☒ General Authorization Form & Fee Transmittal (Submit an original and a duplicate for fee processing)
2. ☒ Specification [Total Pages] 17
   (preferred arrangement set forth below)
   - Descriptive Title of the Invention
   - Cross References to Related Applications
   - Statement Regarding Fed sponsored R & D
   - Reference to Microfiche Appendix
   - Background of the Invention
   - Brief Summary of the Invention
   - Brief Description of the Drawings (if filed)
   - Detailed Description
   - Claim(s)
   - Abstract of the Disclosure
3. ☒ Drawing(s) (35 USC 113) [Total Sheets] 3
4. Oath or Declaration [Total Pages] 1
   - a. □ Newly executed (original or copy)
   - b. ☒ Copy from a prior application (37 CFR 1.63(d)) (for continuation/divisional with Box 17 completed)
     - i. □ DELETION OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b)
5. ☒ Incorporation By Reference (useable if box 4b is checked) The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered to be part of the disclosure of the accompanying application and is hereby incorporated by reference therein.
6. □ Microfiche Computer Program (Appendix)
7. Nucleotide and Amino Acid Sequence Submission (if applicable, all necessary)
   - a. □ Computer-Readable Copy
   - b. □ Paper Copy (identical to computer copy)
   - c. □ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

8. □ Assignment Papers (cover sheet & document(s))
9. ☒ 37 CFR 3.73(b) Statement (when there is an assignee) ☒ Power of Attorney
10. □ English Translation Document (if applicable)
11. ☒ Information Disclosure Statement (IDS)/PTO-1449 □ Copies of IDS Citations
12. ☒ Preliminary Amendment
13. ☒ Return Receipt Postcard
14. □ Small Entity Statement(s) □ Statement filed in prior application, Status still proper and desired
15. □ Certified Copy of Priority Document(s) (if foreign priority is claimed)
16. ☒ Other: Certificate of Express Mail
    Check
    Revocation and Substitute Power of Attorney

17. **If a CONTINUING APPLICATION,** *check appropriate box and supply the requisite information below and in a preliminary amendment*

☒ Continuation □ Divisional □ Continuation-In-Part (CIP) of prior Application No.: 08/909,811 Filed August 12, 1997

Prior application information: Examiner Hieu Le Group / Art Unit 2757

□ Claims the benefit of Provisional Application No. ______

CORRESPONDENCE ADDRESS

Edward W. Bulchis, Esq.
Dorsey & Whitney LLP
1420 Fifth Avenue, Suite 3400
Seattle, Washington 98101-4010
(206) 903-8800 *phone*
(206) 903-8820 *fax*

Respectfully submitted,

TYPED or PRINTED NAME Edward W. Bulchis REGISTRATION NO. 26,847

SIGNATURE Edward W Bulchis Date August 8, 2000

o:\ip\documents\clients\micron electronics\100\500122 02\500122 02 sb05 doc

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Hoyt A. Fleming, III Attorney Docket No.: 500122.02

Filed : August 8, 2000

Title : METHOD AND SYSTEM FOR FILTERING UNAUTHORIZED ELECTRONIC MAIL MESSAGES

CERTIFICATE OF MAILING BY "EXPRESS MAIL"

Box Patent Application
Assistant Commissioner of Patents
Washington, D.C. 20231

Sir:

I hereby certify that the enclosures listed below are being deposited with the United States Postal Service "EXPRESS MAIL Post Office to Addressee" service under 37 C.F.R. § 1.10, Mailing Label Certificate No. EL476400477US, on August 8, 2000, addressed to Box Patent Application, Assistant Commissioner for Patents, Washington, DC 20231.

Respectfully submitted,

DORSEY & WHITNEY LLP

Susan Johnson

West Courier

Enclosures:

Postcard
Check
Form PTO/SB/05
Preliminary Amendment
General Authorization Under 37 C.F.R. § 1.136(a)(3) and Fee Transmittal (+ copy)
Copy of Previously Filed Specification, Claims, Abstract (17 pages)
3 Sheets of Drawings (Figures 1-3)
Copy of Previously Filed Declaration
Copy of Previously Filed Election and Power of Attorney
Revocation and Substitute Power of Attorney
Information Disclosure Statement and Form PTO-1449

EXPRESS MAIL NO.: EL476400477US

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Present Application:

Applicant : Hoyt A. Fleming, III
Attorney Docket No.: 500122.02
Filed : Concurrently herewith
Title : METHOD AND SYSTEM FOR FILTERING UNAUTHORIZED ELECTRONIC MAIL MESSAGES

Prior Application:

Examiner : Hieu Le
Art Unit : 2757
Serial No. : 08/909,811

PRELIMINARY AMENDMENT

Box Patent Application
Assistant Commissioner of Patents
Washington, D.C. 20231

Sir:

Please amend the above-identified application as follows:

In the Specification:

Amend the specification by inserting a new section before the "Technical Field" as follows:

-- CROSS-REFERENCE TO RELATED APPLICATION

This application is a continuation of pending United States Patent Application No. 08/909,811, filed August 12, 1997. --

In the Claims:

Please cancel claims 15 and 18.

REMARKS

Claims 15 and 18 are being cancelled thereby leaving claims 1-14, 16, 17 and 19-28 for examination.

Respectfully submitted,

DORSEY & WHITNEY LLP

Edward W Bulchis

Edward W. Bulchis
Registration No. 26,847

EWB:cff

Enclosures:
Postcard

1420 Fifth Avenue, Suite 3400
Seattle, WA 98101
(206) 903-8800
(206) 903-8820 (facsimile)

o:\ip\documents\clients\micron electronics\100\500122.02\500122.02 prelim doc

METHOD AND SYSTEM FOR FILTERING UNAUTHORIZED ELECTRONIC MAIL MESSAGES

TECHNICAL FIELD

This invention relates generally to electronic mail systems and more particularly to the filtering of electronic mail messages.

BACKGROUND OF THE INVENTION

Electronic mail is becoming an increasingly popular form of communications. Electronic mail systems allow one user of a computer system (*i.e.*, a sender) to send a message electronically to another user (*i.e.*, a recipient). To create an electronic mail message, the sender designates the recipient to whom the electronic mail is to be sent and creates the body (*e.g.*, text) of the electronic mail message. The electronic mail system then forwards the electronic mail message to the recipient via a communications mechanism such as a local area network or the Internet. When the recipient receives the electronic mail messages, the recipient can view the body of the electronic mail message.

To ensure format compatibility among various electronic mail systems, the electronic mail messages are formatted in accordance with a conventional format such as defined by the Simple Mail Transfer Protocol ("SMTP"). According to this format, the electronic mail message contains an envelope portion and a body portion. The envelope portion identifies the sender and the recipient, identifies the electronic mail address of the recipient, and may identify the subject of the electronic mail message. The body portion contains the message itself, which is typically in text format. The electronic mail system may need to route an electronic mail message through various computer systems until it reaches the computer system of the recipient. Each of the computer systems through which the electronic mail message is routed use the recipient's electronic mail address to forward the electronic mail message.

Electronic mail systems store electronic mail messages that have been sent or received in a file referred to as the electronic mail file. The electronic mail files are typically organized into various folders and subfolders. The folders allow a user of the electronic mail system to store related electronic mail messages in the same folder in a way that is very similar to how directories allow a user of a file system to store related files in the same directory. When the electronic mail system receives an electronic mail message for a user, the electronic mail system stores the electronic mail message in a folder that is designated as the "Inbox" folder within the user's electronic mail file. The electronic mail system allows the user to view the electronic mail messages that are currently in the Inbox folder. When the user selects to display the contents of the Inbox folder, the electronic mail system displays information from the envelope portion (*e.g.*, sender's name and subject information) for each of the electronic mail messages currently in the folder. Based on the envelope information, the user can select to display the body of an electronic mail message. The electronic mail system also allows the user to move the electronic mail messages from the Inbox folder to other folders or to delete the electronic mail messages. When a user sends an electronic mail message, the electronic mail system typically saves a copy of the electronic mail message in a folder that is designated as the "Sent" folder. The user can move and delete the electronic mail messages stored in any of the folders in the same manner as done for the Inbox folder.

The electronic mail address for a user uniquely identifies the computer system at which the recipient expects to receive the electronic mail messages. Electronic mail addresses can be very complex strings of characters that identify countries, companies, divisions within companies, and individual users. Thus, to provide a more friendly user interface, typical electronic mail systems maintain an address book that contains a mapping of the names of the users to their electronic mail addresses. Thus, when a user wishes to designate a recipient, the user need only indicate the name of the recipient and the electronic mail system uses the address book to retrieve the electronic mail address for that recipient. A user will generally have a personal address book with the names and electronic mail addresses of those recipients to whom the user normally sends electronic mail messages. In addition, the electronic mail systems typically maintain a global address book that is shared by all users of the electronic mail system. For example, the global address book may contain the names and electronic mail addresses of all the employees of a company. An employee may then store the names and electronic mail addresses of non-employee friends in the employee's own personal address book. When the electronic mail system sends an electronic mail message, it searches the global and personal address books for the electronic mail address of the recipient.

Prior to the popularity of the Internet, a user of an electronic mail system generally received electronic mail messages only from known senders. For example, an employee of a company would receive electronic mail messages only from other employees of the company. The electronic mail system may only be connected to computer systems owned by the company. However, with the increasing popularity of the Internet, a user may be able to send electronic mail messages to anyone who is connected to the Internet. The sender of an electronic mail message needs only to know the electronic mail address of the recipient. Thus, users can and often do receive electronic mail messages from unknown senders.

Recently, a problem has developed which seriously impairs the effectiveness of electronic mail systems. Many large promotional companies are turning to the Internet to advertise products of their clients. These promotional companies acquire and maintain lists of electronic mail addresses for thousands of users. When a client wants to advertise a product, the promotional company will send an electronic mail message to each electronic mail address in its list. A user may occasionally receive an unsolicited electronic mail message from such a promotional company. Such occasional receipt of such electronic mail message, while annoying, does not seriously impair the effectiveness of the electronic mail system. However, because of the perceived benefits of advertising via the Internet, a user may now receive so many unsolicited electronic mail messages on a daily basis, that the unsolicited electronic mail messages vastly outnumber the electronic mails messages received from known senders. The process of sending these promotional electronic mail messages indiscriminately to the various electronic mail addresses by the promotional companies is referred to as "spamming." Because a recipient may receive so many unsolicited (*i.e.*, junk) electronic mail messages, it may be very difficult for the recipient to sort through and determine which electronic mail messages are not junk. Such sorting has been a serious impediment to the effectiveness of the electronic mail systems. The seriousness of the problem has been recognized and legislation has even been proposed that would outlaw such spamming practices. In addition, several litigations have been spawned to force such promotional companies to cease their spamming practices.

One potential solution to the problems resulting from the spamming practices has been tried, but unfortunately has been unsuccessful. A service, known as a "de-spamming service," has been provided that attempts to limit the junk mail that is sent. Such a de-spamming service maintains a list of the electronic mail addresses of users who have requested not to receive junk mail. When a promotional company wishes to send an electronic mail message to all the users whose electronic mail addresses are on its mailing list, the promotional company first sends the electronic mail messages to the de-spamming computer system. The de-spamming computer system checks its list of electronic mail addresses and deletes any of the electronic mail messages that are destined to any electronic mail addresses on its list. The de-spamming computer system then forwards the remaining electronic mail messages onto the recipients. Whenever a recipient does not want to be included on a mailing list, the recipient can notify the de-spamming computer system, which will add the recipient's electronic mail address to the list of electronic mail addresses that are not to receive junk mail.

Recently, however, such de-spamming services have ceased offering the service because it has proved to be uneconomical.

Certain electronic mail systems also allow a user to designate how to automatically handle a received electronic mail message. For example, a user can indicate that all electronic mail messages received from a certain sender can automatically be stored in a designated folder, be deleted, or be forwarded to another recipient. To provide such routing of electronic mail messages, the user needs to specify a characteristic (*e.g.*, sender = John Smith) of the envelope portion or the body portion so that the electronic mail system can determine which electronic mail systems satisfy the characteristic. However, with such electronic mail systems, a user cannot specify how to automatically handle electronic mail messages if they are unaware of any characteristic of the electronic mail message. In particular, a user may not know in advance the identity of the sender of junk mail and thus cannot have the junk mail automatically deleted.

SUMMARY OF THE INVENTION

Some embodiments of the present invention provide a computer system and method for filtering unauthorized messages that are received by a user. For each message received, the system determines whether the sender of the message is designated as being authorized to send messages to the user. When the sender of the message is determined to be authorized, the system indicates that the message is from an authorized sender. When the sender of the message is determined to be not authorized, the system indicates that the message is from an unauthorized sender. In this way, the recipient (*i.e.*, the user) of the messages can identify whether a message is authorized based solely on the indications. In one embodiment, the messages are electronic mail messages, and the system provides the indications by storing the filtered electronic mail messages in separate folders. The system also maintains a list of authorized senders that it uses when determining whether the sender of the message is designated as being authorized. In another aspect of the present invention, the system automatically adds each recipient of an electronic mail message sent by a user to the list of senders who are authorized to send electronic mail messages to that user.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram illustrating a computer system for practicing the present invention.

Figure 2 is a flow diagram of a routine that provides an implementation of the authorizing for the authorization component.

Figure 3 is a flow diagram of a routine that provides an implementation of the automatic updating of the authorized senders list.

DETAILED DESCRIPTION OF THE INVENTION

The present invention provides a method and system for filtering electronic mail messages that are received from unauthorized senders. In one embodiment of the present invention, an authorization component is included with an electronic mail system. The authorization component intercepts electronic mail messages that are sent to a user before they are placed in the user's Inbox folder. The authorization component has the identifications of all senders who are authorized to send electronic mail messages to the user. When an electronic mail message is intercepted, the authorization component retrieves the identification of the sender from the envelope portion of the intercepted electronic mail message. The authorization component then determines whether the retrieved identification of the sender matches the identification of one of the authorized senders. If the retrieve identification does not match, then the authorization component stores the intercepted electronic mail message in a pre-designated location, such as a "Junk Mail" folder. Otherwise, the authorization component forwards the intercepted electronic mail message to the electronic mail system for normal processing and storage. With the use of such an authorization component a user can effectively filter out unauthorized (*i.e.*, junk) electronic mail messages. Periodically, the user can view the Junk Mail folder to delete or read the electronic mail messages that were designated as junk.

The authorization component can store the identifications of the authorized senders in a list that is either manually or automatically updated. A user can manually update the authorized sender list in several circumstances. For example, when an electronic mail message is stored in the Junk Mail folder but the user does not consider the electronic mail message to be junk, the user can add the identification of the sender to the authorized sender list. Conversely, when an electronic mail message is not stored in the Junk Mail folder but the user considers the electronic mail message to be junk, the user can remove the identification of the sender from the authorized sender list. The authorization component can also automatically update the authorized sender list in several circumstances. For example, the authorization component can scan previously sent electronic mail messages and add the identifications of the recipients to the authorized sender list. The authorization component can also scan previously received electronic messages (*e.g.*, in a certain folder) and add the identifications of the senders to the authorized sender list. In addition, the authorization component can automatically add the identification of each recipient to the authorized sender list whenever the user sends an electronic mail message. The authorization component can also allow the user to disable the filtering of electronic mail messages. It may be desirable to disable such filtering, for example, when the authorized sender list has not yet been updated to contain the identification of most of the authorized senders.

The authorization component can be used by an administrator of an electronic mail system of a company to ensure that the employees do not receive unauthorized electronic mail messages. For example, the administrator could maintain a global authorized sender list that is shared by all employees. The authorized sender list could contain only the names of the employees of the company. If the authorization component automatically deleted the electronic mail messages from senders not in the authorized sender list, then the employees would only receive electronic mail messages sent by other employees. Alternatively, the global authorized sender list can serve to relieve each individual employee of maintaining an authorized sender list with the names of all employees. Each employee could also maintain a personal authorized sender list that identifies additional senders (*e.g.*, spouse) who are authorized to send electronic mail messages to the employee. The authorization component would only consider an electronic mail message to be junk when the identification of the sender is not in either the global or the personal authorized sender list. A user may be allowed to specify and de-specify many different authorized sender lists at various times. For example, a user may have an authorized sender list for business acquaintances and another authorized sender list for social acquaintances.

The authorization component can handle the electronic mail message from unauthorized senders in different ways other than automatically storing in a Junk Mail folder or deleting. For example, electronic mail messages received from a sender who is not an employee of a company can automatically be routed to the electronic mail system administrator. Also, all electronic mail messages from unauthorized senders can be automatically forwarded to an assistant of the user who can determine whether the electronic mail message is really junk. If the electronic mail message is not junk, then the assistant can re-send the electronic mail message to the user and update the authorized sender list for the user accordingly. Also, the authorization component can simply store an indication that indicates whether or not an electronic mail message is from an authorized sender. When the electronic mail system displays electronic mail messages, it can display a visual indicator as to whether each electronic mail message is junk based on the stored indication. For example, the visual indication could be the displaying of information relating to the junk electronic mail messages in a dimmer intensity than the non-junk electronic mail messages.

Figure 1 is a block diagram illustrating a computer system for practicing the present invention. The computer system 100 includes memory 101, central processing unit 102, I/O interface 103, display device 104, and electronic mail connection 109. The memory contains the electronic mail system 105 which includes the authorization component 106 of the present invention. The electronic mail system passes each electronic mail message it receives to the authorization component. The authorization component uses the authorized sender list 108 to determine whether the sender of the electronic mail message is authorized to send the received electronic mail message. If the sender is not authorized, the authorization component stores the received electronic mail message in a designated Junk Mail folder in the electronic mail file 107. The authorization component can operate as an add-on component to any system (*e.g.*, Internet browsers) that supports the receiving of electronic mail messages.

Figure 2 is a flow diagram of a routine that provides an implementation of the authorizing for the authorization component. This routine receives the authorized sender list and the electronic mail messages. The routine determines whether the identification of the sender of each electronic mail message is in the authorized sender list. If the sender is authorized, then the routine stores the electronic mail message in a designated folder for authorized senders. If the sender is not authorized, then the routine stores the electronic mail message in a Junk Mail folder. In step 201, the routine selects the next electronic mail message starting with the first. In step 202, if all the electronic mail messages have already been selected, then the routine is complete, else the routine continues at step 203. In step 203, the routine retrieves the identification of the sender of the selected electronic mail message. In step 204, if the retrieved identification is in the authorized sender list, then the routine continues at step 205, else the routine continues at step 206. In step 205, the routine stores the selected electronic mail message in the Inbox folder and loops to step 201 to select the next electronic mail message. In step 206, the routine stores the selected electronic mail message in the Junk Mail folder and loops to step 201 to select the next electronic mail message.

Figure 3 is a flow diagram of a routine that provides an implementation of the automatic updating of the authorized sender list. This flow diagram shows the portion of the authorization component that adds the recipients of a sent electronic mail message to the authorized sender list for the sender of the electronic mail message. The ellipsis shown in the figure indicates conventional processing to send an electronic mail message. In step 301, the routine retrieves the identification of the next recipient of the electronic mail message to be sent starting with the first. In step 302, if the identifications of all the recipients of the electronic mail message to be sent have already been selected, then the routine continues with the sending of the electronic mail message, else the routine continues at step 303. At step 303, if the retrieved identification is already in the authorized sender list, then the routine loops to step 301 to retrieve the identification of the next recipient, else the routine continues at step 304. In step 304, the routine adds the retrieved identification to the authorized sender list and loops to step 301 to select the next recipient.

From the foregoing it will be appreciated that, although specific embodiments of the invention have been described herein for purposes of illustration, various modifications may be made without deviating from the spirit and scope of the invention. Accordingly, the invention is not limited except as by the appended claims.

CLAIMS

1. A method in a computer system for filtering unauthorized electronic mail messages that are sent by senders to a user, each sender having an identification, each electronic mail message including the identification of the sender, the method comprising:

providing a list of the identifications of the senders who are authorized to send an electronic mail message to the user;

for each of a plurality of electronic mail messages,

determining whether the sender of the electronic mail message is authorized by determining whether the identification of sender in the electronic mail message is in the provided list of the identifications of the senders who are authorized;

when the sender of the electronic mail message is determined to be authorized, storing the electronic mail message in a first folder designated for electronic mail messages received from authorized senders;

when the sender of the electronic mail message is determined to be not authorized, storing the electronic mail message in a second folder designated for electronic mail messages received from unauthorized senders

whereby the electronic mail messages are automatically stored in the appropriate folder based on whether the sender is authorized so that the user can view the first folder containing the electronic mail messages sent by authorized senders separately from the second folder containing the electronic mail messages sent by unauthorized senders.

2. The method of claim 1 wherein when the user sends an electronic mail message to a recipient, the identification of the recipient is automatically added to the provided list of the identifications of senders who are authorized to send electronic mail message to the user.

3. The method of claim 1 wherein the provided list of the identifications of the senders is generated by adding the identification of senders of previously received electronic mail messages.

4. The method of claim 1 wherein the provided list of the identifications of the senders is generated by adding the identification of recipients of previously sent electronic mail messages.

5. A method in a computer system for filtering unauthorized messages, each message having a sender, the method comprising:

for each of a plurality of messages,

determining whether the sender of the message is designated as being authorized;

when the sender of the message is determined to be authorized, indicating that the message is from an authorized sender; and

when the sender of the message is determined to be not authorized, indicating that the message is from an unauthorized sender.

6. The method of claim 5 wherein the recipient of the messages can identify whether a message is authorized based solely on the indications.

7. The method of claim 5 wherein the message is indicated as authorized by storing in a pre-designated location for messages sent by authorized senders.

8. The method of claim 7 wherein the message is an electronic mail message and the pre-designated location is a folder.

9. The method of claim 5 including when displaying a list of messages, displaying a visual indication as to whether the message has been indicated as being sent from an authorized or unauthorized sender.

10. The method of claim 9 wherein the visual indication is the dimming of the messages that are sent from unauthorized senders in the list of messages.

11. The method of claim 5 wherein the computer system includes a list of authorized senders and wherein the determining whether the sender of the message is designated as being authorized includes determining whether the sender is in the list of authorized senders.

12. The method of claim 11 wherein the list of authorized senders is generated by adding the senders of the previously received messages to the list.

13. The method of claim 11 wherein the list of authorized senders is generated by adding the recipients of the previously sent messages to the list.

14. The method of claim 11 wherein the list is shared by multiple users.

15. The method of claim 14 wherein the computer system includes a personal list of authorized senders that is personalized to the recipient and wherein a messages is determined to be sent by a sender designated as unauthorized when the sender is not in either list.

16. The method of claim 11 wherein when the recipient sends a message to an intended recipient, the intended recipient is added to the list as an authorized sender.

17. The method of claim 5 wherein the indicating that the message is from an unauthorized sender includes forwarding the message to another user.

18. The method of claim 17 wherein the other user sends a forwarded message back to the recipient when the message should be viewed by the recipient even though the sender is not authorized.

19. The method of claim 5 wherein the indicating that the message is from an unauthorized sender includes deleting the message.

20. An electronic mail system comprising:

a receiving component that receives electronic mail messages that include the identification of the sender of the electronic mail message;

an authorized sender list having the identification of senders who are authorized to send electronic mail messages; and

an authorization component that is forwarded electronic mail messages from the receiving component and that provides an indication when the identification of the sender of the forwarded electronic mail message is not in the authorized sender list.

21. The system of claim 20 including an updated authorized sender list component that adds the identification of each recipient of sent electronic mail messages to the authorized sender list.

22. The system of claim 20 including an updated authorized sender list component that scans previously received electronic mail messages and adds the identification of the sender to the authorized sender list.

23. The system of claim 20 wherein the provided indication is the storing of the forwarded electronic mail message in a junk mail folder.

24. The system of claim 20 wherein the provided indication is the deletion of the forwarded electronic mail message.

25. A method in a computer system for filtering unauthorized electronic mail messages that are sent by senders to a user, each sender having an identification, each electronic mail message including the identification of the sender, the method comprising:

providing a list of the identifications of the senders who are authorized to send an electronic mail message to the user;

for each of a plurality of electronic mail messages,

determining whether the sender of the electronic mail message is authorized by determining whether the identification of sender in the electronic mail message is in the provided list of the identifications of the senders who are authorized;

when the sender of the electronic mail message is determined to be authorized, storing the electronic mail message in a first folder designated for electronic mail messages received from authorized senders;

when the sender of the electronic mail message is determined to be not authorized, storing the electronic mail message in a second folder designated for electronic mail messages received from unauthorized senders whereby the electronic mail messages are automatically stored in the appropriate folder based on whether the sender is authorized so that the user can view the first folder containing the electronic mail messages sent by authorized senders separately from the second folder containing the electronic mail messages sent by unauthorized senders.

26. The method of claim 25 wherein when the user sends an electronic mail message to a recipient, the identification of the recipient is automatically added to the provided list of the identifications of senders who are authorized to send electronic mail message to the user.

27. The method of claim 25 wherein the provided list of the identifications of the senders is generated by adding the identification of senders of previously received electronic mail messages.

28. The method of claim 25 wherein the provided list of the identifications of the senders is generated by adding the identification of recipients of previously sent electronic mail messages.

METHOD AND SYSTEM FOR FILTERING UNAUTHORIZED ELECTRONIC MAIL MESSAGES

ABSTRACT OF THE DISCLOSURE

A computer system and method for filtering unauthorized electronic mail messages that are sent by senders to a user. The system includes a list of the identifications of the senders who are authorized to send an electronic mail message to the user. When an electronic mail message is received, the system determines whether the sender of the electronic mail message is authorized by determining whether the identification of sender in the electronic mail message is in the list of the identifications of the senders who are authorized. When the sender of the electronic mail message is determined to be authorized, the system stores the electronic mail message in an Inbox folder. When the sender of the electronic mail message is determined to be not authorized, the system stores the electronic mail message in a Junk Mail folder. In this way, the electronic mail messages are automatically stored in the appropriate folder based on whether the sender is authorized so that the user can view the Inbox folder containing the electronic mail messages sent by authorized senders separately from the Junk Mail folder containing the electronic mail messages sent by unauthorized senders.

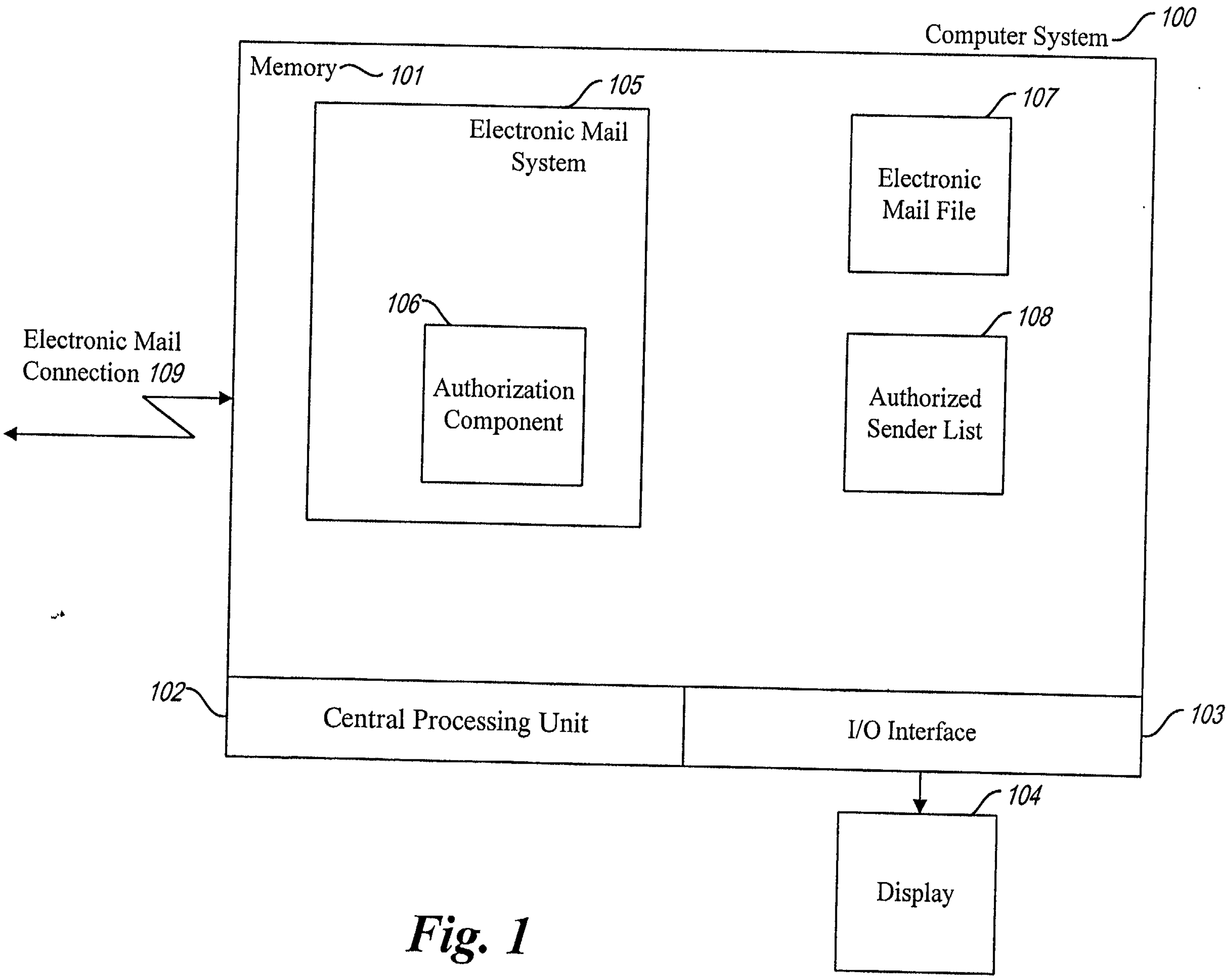
Computer System
100
Memory
101
105
Electronic Mail System
106
Authorization Component
107
Electronic Mail File
108
Authorized Sender List
Electronic Mail Connection 109
102
Central Processing Unit
I/O Interface
103
104
Display

Fig. 1

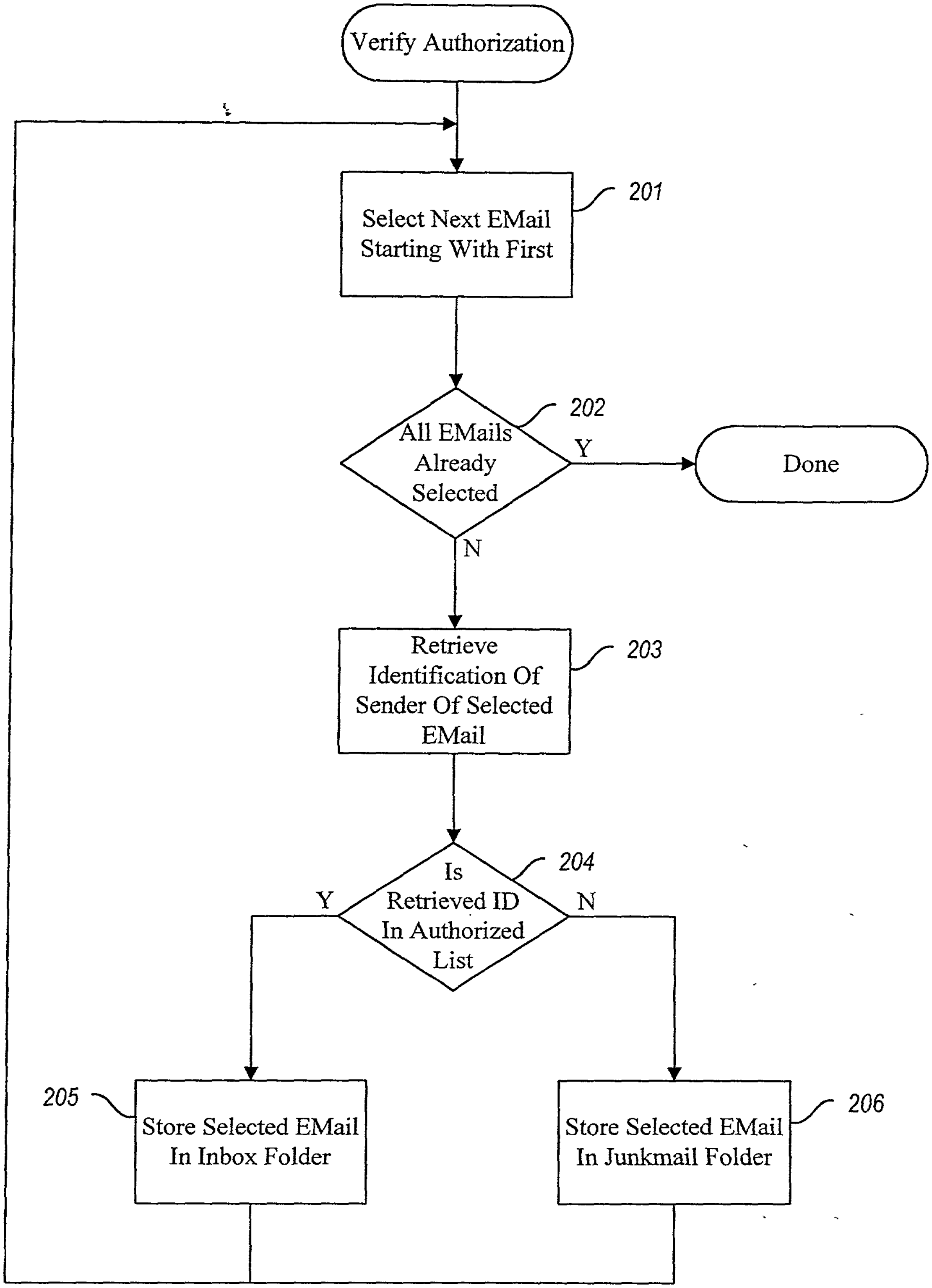
Verify Authorization
Select Next EMail Starting With First
201
All EMails Already Selected
202
Y
Done
N
Retrieve Identification Of Sender Of Selected EMail
203
Is Retrieved ID In Authorized List
204
Y
N
205
Store Selected EMail In Inbox Folder
Store Selected EMail In Junkmail Folder
206

Fig. 2

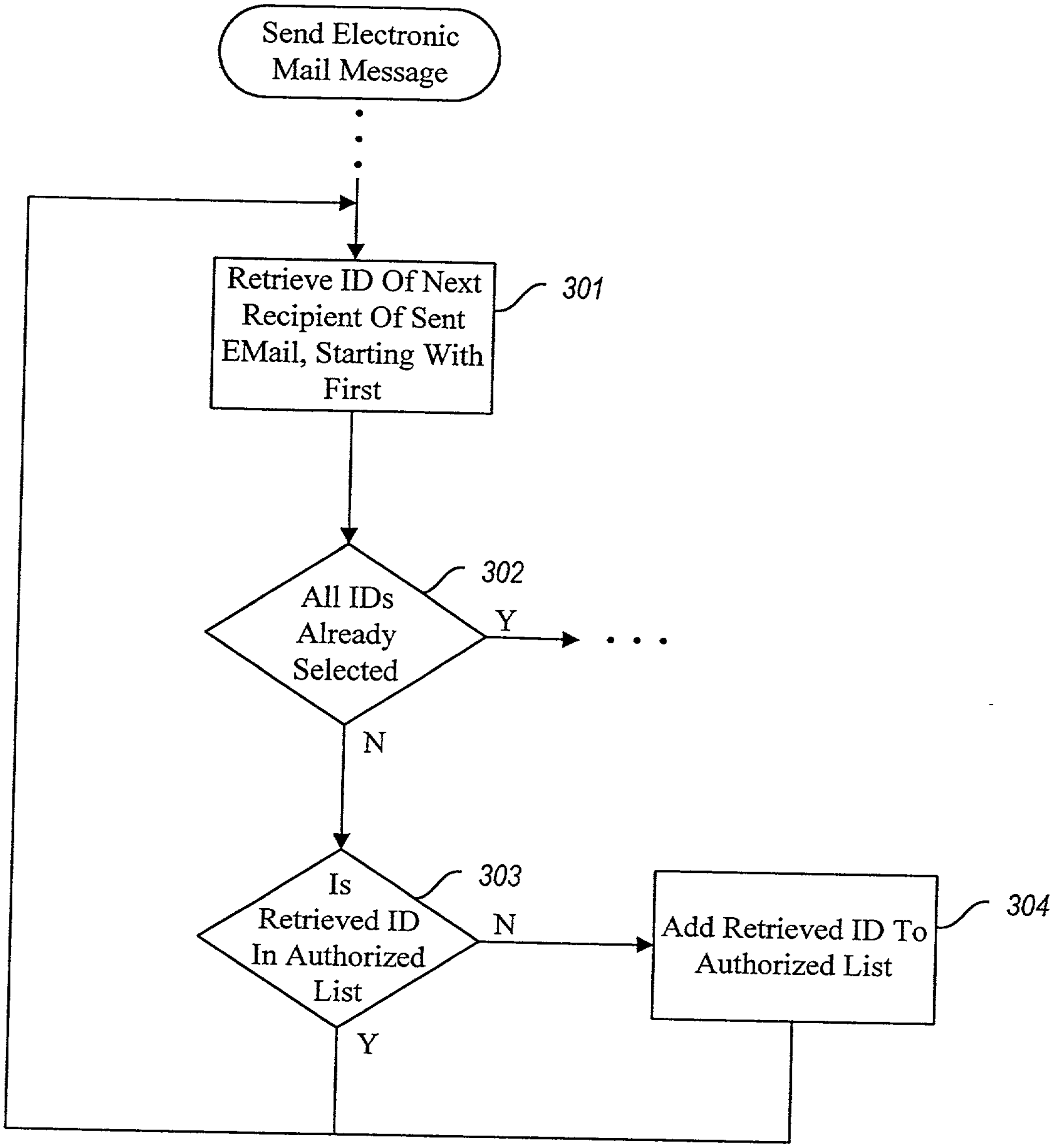
Send Electronic Mail Message
Retrieve ID Of Next Recipient Of Sent EMail, Starting With First
301
All IDs Already Selected
302
Y
N
Is Retrieved ID In Authorized List
303
N
Add Retrieved ID To Authorized List
304
Y

Fig. 3

DECLARATION

As the below-named inventor, I declare that:

My residence, post office address, and citizenship are as stated below under my name.

I believe I am the original, first, and sole inventor of the invention entitled "METHOD AND SYSTEM FOR FILTERING UNAUTHORIZED ELECTRONIC MAIL MESSAGES," which is described and claimed in the specification and claims of Patent Application No. 08/909,811, which was filed in the United States Patent and Trademark Office on August 12, 1997 and for which a patent is sought.

I have reviewed and understand the contents of the above-identified specification and claims, as amended by any amendment specifically referred to herein (if any).

I acknowledge my duty to disclose information of which I am aware which is material to the examination of this application in accordance with 37 C.F.R. § 1.56(a).

I further declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further, that these statements were made with the knowledge that the making of willfully false statements and the like is punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and may jeopardize the validity of any patent issuing from this patent application.

Hoyt A. F[illegible] III

Hoyt A. Fleming III

Date 1/27/98

Residence : City of Boise, County of Ada
State of Idaho

Citizenship : United States of America

P.O. Address : 4134 West Quail Ridge Drive
Boise, Idaho 83703

EXPRESS MAIL NO.: EL476400477US

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	:	Hoyt A. Fleming III
Filed	:	August 12, 1997
Serial No.	:	08/909,811
For	:	METHOD AND SYSTEM FOR FILTERING UNAUTHORIZED ELECTRONIC MAIL MESSAGES

Docket No.	:	660082.476
Date	:	February 15, 1998

Assistant Commissioner for Patents
2011 Jefferson Davis Highway
Washington, DC 20231

ELECTION UNDER 37 C.F.R. §§ 3.71 AND 3.73 AND POWER OF ATTORNEY

Sir:

The undersigned, being Assignee of the entire interest in the above-identified application by virtue of an Assignment filed concurrently herewith, hereby elects, under 37 C.F.R. § 3.71, to prosecute the application to the exclusion of the inventor.

Assignee hereby appoints RICHARD W. SEED, Registration No. 16,557; ROBERT J. BAYNHAM, Registration No. 22,846; EDWARD W. BULCHIS, Registration No. 26,847; GEORGE C. RONDEAU, JR., Registration No. 28,893; DAVID H. DEITS, Registration No. 28,066; WILLIAM O. FERRON, JR., Registration No. 30,633; PAUL T. MEIKLEJOHN, Registration No. 26,569; DAVID J. MAKI, Registration No. 31,392; RICHARD G. SHARKEY, Registration No. 32,629; DAVID V. CARLSON, Registration No. 31,153; MAURICE J. PIRIO, Registration No. 33,273; KARL R. HERMANNS, Registration No. 33,507; DAVID D. McMASTERS, Registration No. 33,963; ROBERT IANNUCCI, Registration No. 33,514; MICHAEL J. DONOHUE, Registration No. 35,859; CHRISTOPHER J. DALEY-WATSON, Registration No. 34,807; STEVEN D. LAWRENZ, Registration No. 37,376; ROBERT G. WOOLSTON, Registration No. 37,263; ELLEN M.

BIERMAN, Registration No. 38,079; BRYAN A. SANTARELLI, Registration No. 37,560; CAROL NOTTENBURG, Registration No. 39,317; CRAIG S. JEPSON, Registration No. 33,517; PAUL T. PARKER, Registration No. 38,264; JOHN C. STEWART, Registration No. 40,188; ROBERT W. BERGSTROM, Registration No. 39,906; DAVID W. PARKER, Registration No. 37,414; ROBERT E. MATES, Registration No. 35,271; BRIAN G. BODINE, Registration No. 40,520; FRANK ABRAMONTE, Registration No. 38,066; E. RUSSELL TARLETON, Registration No. 31,800; FREDERICK M. FLIEGEL, Registration No. 36,138; JAN C. L. MAXWELL, Registration No. 41,181; THOMAS L. EWING, Registration No. 34,328; CLIFTON G. GREEN, Registration No. 41,044; PHILLIP B. C. JONES, Registration No. 38,195; and KEVIN S. COSTANZA, Registration No. 37,801, comprising the firm of SEED AND BERRY LLP, 6300 Columbia Center, Seattle, Washington 98104-7092; along with STEVEN P. ARNOLD, Registration No. 33,354, of Micron Electronics, Inc., 900 East Karcher Road, Nampa, Idaho 83687, as its attorneys to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. Please direct all telephone calls to Maurice J. Pirio at (206) 622-4900 and telecopies to (206) 682-6031.

Please direct all communications to:

Maurice J. Pirio, Esq.
Seed and Berry LLP
6300 Columbia Tower
701 Fifth Avenue
Seattle, Washington 98104-7092

Pursuant to 37 C.F.R. § 3.73, the undersigned duly authorized designee of Assignee certifies that the evidentiary documents have been reviewed, specifically the Assignment to MICRON ELECTRONICS, INC., filed concurrently herewith for recording, a copy of which is attached hereto, and certifies that to the best of my knowledge and belief, title remains in the name of the Assignee.

MICRON ELECTRONICS, INC.
ASSIGNEE

1/27/98
DATE

III

Enclosure:
Copy of Assignment

EXPRESS MAIL NO EL476400477US

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Hoyt A. Fleming, III Attorney Docket No.: 500122.02

Filed : August 8, 2000

Title : METHOD AND SYSTEM FOR FILTERING UNAUTHORIZED ELECTRONIC MAIL MESSAGES

TRANSMITTAL FOR REVOCATION AND SUBSTITUTE POWER OF ATTORNEY

Box Patent Application
Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Transmitted herewith and attached hereto as Addendum A is a true and correct copy of the Revocation and Substitute Power of Attorney executed February 7, 2000, in the above-identified application. The above-identified application is identified on Exhibit A.

Pursuant to 37 C.F.R. § 3.73, Paul A. Revis, duly authorized designee of Assignee, has certified that the evidentiary documents have been reviewed, specifically the Assignment to MICRON ELECTRONICS, INC., recorded under Reel 9002 / Frame 0850,and certified that to the best of his knowledge and belief, title remains in the name of the Assignee.

Respectfully submitted,

DORSEY & WHITNEY LLP

Edward W Bulchis

Edward W. Bulchis
Registration No. 26,847

EWB:cff

Enclosures:
Addendum A
Exhibit A

1420 Fifth Avenue, Suite 3400
Seattle, Washington 98101-4010
(206) 903-8800 (telephone)
(206) 903-8200 (fax)

o.\ip\documents\clients\micron electronics\100\500122 02\500122 02 rev poa.doc

ADDENDUM A

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

REVOCATION AND SUBSTITUTE POWER OF ATTORNEY

Assistant Commissioner of Patents
Washington, D.C. 20231

Sir:

In the matter of the patent application identified in Exhibit A attached hereto, I, PAUL A. REVIS, declare that I am a duly authorized designee of Micron Electronics, Inc., the ASSIGNEE of the entire right, title and interest in and to the patent application identified in Exhibit A attached hereto. Pursuant to 37 C.F.R. § 3.73, I certify that Documentary evidence of chain of title from the original owner to ASSIGNEE has been or is concurrently being filed with and recorded by the United States Patent Office. The evidentiary documents referred to in the instant Revocation and Power of Attorney have been reviewed by the undersigned, and it is certified that, to the best of ASSIGNEE's knowledge and belief, title is held solely in and by ASSIGNEE.

On behalf ASSIGNEE, I revoke all power of attorney heretofore given, and hereby appoint EDWARD W. BULCHIS, Reg. No. 26,847; JON F. TUTTLE, Reg. No. 25,713; PAUL T. MEIKLEJOHN, Reg. No. 26,569; GLENN P. RICKARDS, Reg. No. 29,428; DALE C. BARR, Reg. No. 40,498; KIMTON N. ENG, Reg. No. 43,605; DAVID E. BOONE, Reg. No. 27,857; SCOTT W. DOYLE, Reg. No. 39,176; REED R. HEIMBECHER, Reg. No. 36,353; JOHN T. KENNEDY, Reg. No. 42,717; GREGORY D. LEIBOLD, Reg. No. 36,408; GARY M. POLUMBUS, Reg. No. 25,364; THOMAS H. YOUNG, Reg. No. 25,796; W. ROBINSON H. CLARK, Reg. No. 41,530; GREGORY J. GLOVER, Reg. No. 34,173; JOHN K. HARROP, Reg. No. 41,817; CHRIS McWHINNEY, Reg. No. 42,875;

ALDO NOTO, Reg. No. 35,628; MATTHEW PHILLIPS, Reg. No. 43,403; JOHN W. RYAN, Reg. No. 33,771; AMI P. SHAH, Reg. No. 42,143; SEAN S. WOODEN, Reg. No. 43,997; MICHAEL C. GILCHRIST, Reg. No. 40,619; BRIAN J. LAURENZO, Reg. No. 34,207; SHANE COLEMAN, Reg. No. 44,623; RONALD J. BROWN, Reg. No. 29,016; DAVID E. BRUHN, Reg. No. 36,762; DAVID N. FRONEK, Reg. No. 25,678; JOSEPH F. HAAG, Reg. No. 42,612; STUART R. HEMPHILL, Reg. No. 28,084; GRANT A. JOHNSON, Reg. No. 42,696; KENNETH E. LEVITT, Reg. No. 39,747; NIALL A. MACLEOD, Reg. No. 41,963; SCOTT A. MARKS, Reg. No. 44,902; DEVAN V. PADMANABHAN, Reg. No. 38,262; GERALD H. SULLIVAN, Reg. No. 36,311; BRIAN PARK, Reg. No. P-45,519; MARK W. ROBERTS, Reg No. P-46,160; STEVEN H. ARTERBERRY, Reg. No. P-46,314; of the firm of DORSEY & WHITNEY LLP, along with HOYT A. FLEMING III, Reg. No. 41,752; and PAUL A. REVIS, Reg. No. 45,040, of Micron Electronics, Inc., 900 East Karcher Road, Nampa, Idaho 83687, as its attorneys to transact all business in the Patent and Trademark Office connected therewith.

Please direct all future correspondence and telephone calls to:

Edward W. Bulchis, Esq.
DORSEY & WHITNEY LLP
U.S. Bank Centre, Suite 3400
1420 Fifth Avenue
Seattle, Washington 98101-4010
(206) 903-8800
(206) 903-8820 facsimile.

ASSIGNEE:

Micron Electronics, Inc.

2/7/0
Date

By
Paul A. Revis
Intellectual Property Counsel

Enclosure:
Exhibit A

O:\IP\Forms\Clients\Micron Electronics 361596\rev sub poa.doc

Exhibit A

Appl. No.	Atty Dkt #	Applicants	Filed	Title
08/909,811	660082.476	Hoyt A. Fleming, III	12-Aug-97	Method and System for Filtering Unauthorized Electronic Mail Messages
Not yet assigned	500122.02 (660082.476C1)	Hoyt A. Fleming, III	Concurrently Herewith	Method and System for Filtering Unauthorized Electronic Mail Messages